

科技ABC人才发展系列

CYBERSECURITY

网络安全人才发展：

亚太地区创新与招聘趋势

亚太地区网络
安全专家洞见

热门招聘
趋势

2021年及未来网络
安全技术创新趋势

网络安全人才招聘
的实用技巧

VISIT...

LANZAROTE
Caliente.COM

新冠肺炎疫情对全球网络安全领域的影响



受新冠疫情影响，
网络犯罪率

上升 **600%**



据微软统计，2020年2月至5月，微软在亚洲地区共监测到

1900万

次勒索软件和钓鱼网站攻击，其中多以冠状病毒为主题



74%

的企业将提升网络安全视为首要任务



受新冠疫情影响，

69%

的企业对其网络安全响应计划做出调整

市场规模

2019年，亚太地区的网络安全市场规模为**304.5亿美元**。

预计2020年至2025
将达到18.3%。



预计受网络安全漏洞影响最严重的行业



金融服务与银行



电子商务

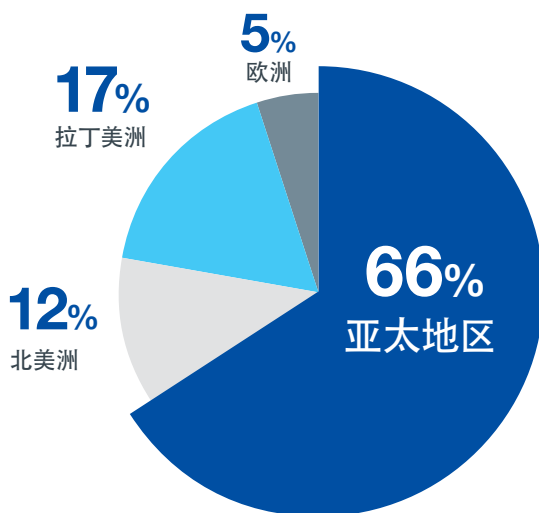


医疗保健与生命科学

职位速览

全球的网络安全人才
缺口达到

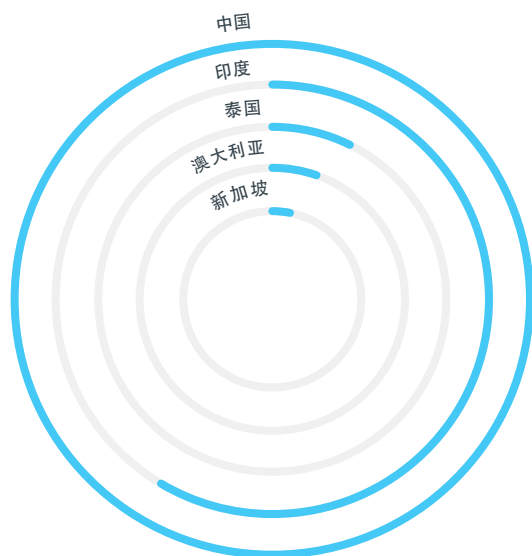
350万



据ISACA统计，招聘网络安全人才平均需要耗时

3至6个月

全球各国网络安全职位预测



到2025年, 各国新增就业岗位

中国	2,686,020
印度	1,508,536
泰国	115,588
澳大利亚	39,923
新加坡	8,769

网络安全人才招聘的主要挑战



43% 人才紧缺



25% 薪酬预算限制



22% 求职者技能存在差距

亟需技能

访问管理 云安全 健康数据安全
合规与控制 威胁情报
应用开发安全 安全策略与治理
数据隐私与安全 风险管理 事件响应

全球网络安全人才



31% 的新招网络安全人才是顾问或灵活人才



66% 的网络安全专业人员无明确的职业发展规划



60% 的网络安全专业人员对现有工作不满

参考资料

<https://purplesec.us/resources/cyber-security-statistics/#:-:text=Cyber%20Security%20Risks,and%20health%20records%20left%20unprotected.>
<https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market>
<https://www.crowdstrike.com.au/wp-content/uploads/2020/07/CrowdStrike-APJ-Survey-Summary.pdf>
<https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B>
<https://www.darkreading.com/cloud/it-takes-an-average-of-3-to-6-months-to-fill-a-cybersecurity-job/d/d-id/1334135>
<https://www.isaca.org/go/state-of-cybersecurity-2020>
<https://msit.powerbi.com/view?r=eyJrJoiZWMyNjA0YzAtZGY4Zi00MTI1LTk4MjQ0NW11NTA5NDY1MzRjliwidCI6IjcyZjk4OGJmLTg2ZjEtNDNFhZi05MWFhLTJkN2NmMDEExZGI0NyIsImMiOiV9>
https://www.burning-glass.com/wp-content/uploads/2020/10/Fastest_Growing_Cybersecurity_Skills_Report.pdf
<https://www.esg-global.com/hubfs/ISSA/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf>

2020年7月15日，45位知名人士的推特账户同时发布了一条令人难以置信且极具诱惑力的可疑推文，内容涉及比特币交易方案。奥巴马、比尔·盖茨、杰夫·贝索斯、埃隆·马斯克和沃伦·巴菲特等账户发布的这条信息称，作为一项精心设计的慈善活动的一部分，在接下来30分钟内，任何人只要把比特币转到某个指定加密货币钱包，就能得到双倍奉还。在此之后的数分钟内，该账户产生了320笔比特币交易，金额总计超过11万美元。

然而，这条推文实际上是一个比特币骗局，并在后来被认为是“社交媒体平台迄今为止最糟糕的黑客事件”。三名涉案罪犯很快被捕，其中主谋是来自佛罗里达州的一名17岁青少年。

这并非2020年唯一的一起重大数据泄露事件。同年3月，万豪国际520多万名酒店入住客人的私人信息被盗；4月，50多万Zoom账户密码被以单价不到一美分的价格出售；2019年1月，新加坡卫生部14200名确诊艾滋病病人的保密信息外泄，这是六个月内的第二起重大健康数据泄露事件。虽然网络安全已经日益成为全球企业面临的挑战，但是更令人担忧的事实是，大部分企业——约95%——并没有实施足够的网络安全实践，因而更容易受到攻击。

布局技术当然是个好的开始，不过填补网络安全空缺的最佳方法之一是聘请市场上优秀的网络安全人才，而与之相关的技能又有哪些呢？网络安全趋势和威胁不断发展变化，企业应该聘用哪类人才呢？

为了解决这些迫在眉睫的问题，米高蒲志访谈亚太地区的商业领袖、学者和公司内部咨询顾问，获得了以下洞见。

网络安全热门创新趋势

1

网络安全威胁日益复杂



过去20年来，网络安全威胁发生了显著变化。“2000年左右最担心的是病毒，因为病毒会攻击电脑的应用程序。”上市公司Vantage Point Security印尼总经理Faisal Yahya回忆说。不过，随着恶意软件、勒索软件、钓鱼软件和SQL注入等网络攻击方式的出现，网络安全的复杂性与日俱增。

“企业为了防护所有资产不得不在网络安全上进行大量投资，但是只需要一次攻击就会让你的网络安全管理前功尽弃。”澳大利亚联邦科学与工业研究组织（CSIRO）Data61首席科学家兼Data61分布式系统安全部门课题组长Surya Nepal说。“解决方案需要结合计算机科学和行为转变等多个学科的综合方法。”不过，Nepal承认并没有万全之策，网络安全威胁绝不会消失，“除非我们不再联网。”

企业欣然接受数字化运作方式，（但是）风险和暴露程度也相应的增加了。”他说。“如果你反应不够灵敏，而且不加控制，只是一味地扩大数字化规模，就可能会面临更多网络相关的风险。”

“在谈到安全问题时，我们不能再把它看成是一个来自外部的威胁。现在我们应该把它看成是一个网状结构，就像蜘蛛网一样。”Yahya补充道。这对网络安全专业人员来说是一个重大挑战，因为它意味着网络安全措施不能只固守于一个安全的位置，现在它必须守护每一处，事无巨细。

深信服科技股份有限公司首席安全架构师阮有明认为中国大陆也存在同样的趋势。“边界防护的作用在新的安全问题面前已经失去优势。网络边界正在消失，单纯地建立防火墙难以维继。”他说。“相反，建立终身防御体系才是新的趋势，就是讲究多个产品之间的联动防御，从而增强整个系统的防御能力。”

2

网络安全的去中心化



网络安全曾经很简单。只需要把你保护的东西放在电脑或服务中，然后围绕它们建立起虚拟墙或者防火墙。正如Yahya所说，这种方式就像四面带有城墙的中世纪城堡一样，保护最重要的资产。

不过，过去十年来，5G、物联网和云计算等科技的发展让上述概念变得过时，因为连接到同一网络的设备越多，就意味着可攻击的潜在端点也越多。新冠肺炎疫情迫使企业员工集体将办公设备带回家，这同样也加速网络安全的去中心化。“现在你的家庭网络连接成了企业网络的一部分。”Hack in the Box（HITB）创始人兼首席执行官、HITB年度安全大会的幕后组织者Dhillon Andrew Kannabhiran说。“你的企业网络会接触到更多设备，比如我家的网络连着智能电视和智能冰箱。企业并没有正确地考虑这些东西。没人做到，真的。”

去中心化趋势也不仅仅只出现在新冠肺炎疫情期间。Viren Parekh是印度制药公司Cipla企业风险管理团队的副总裁。如果没有适当的控制，数字化转型也会让企业更容易遭受攻击。”

“网络安全的投入应该循序渐进，而不是一劳永逸。首先考虑：‘你要保护哪些资产？’和‘对你来说什么重要？’，然后围绕这两个问题来制定策略。”



Surya Nepal

澳大利亚联邦科学与工业研究组织（CSIRO）Data61首席科学家兼Data61分布式系统安全部门课题组长

3 网络安全正在云化



网络安全分析和检测工作过去一向是劳动密集型工种，但是 阮有明发现这些工作正在更多地向云端迁移，其自动化程度在逐步提升。

在自动化方面，人工智能现在能够检测黑客流量特征和行为特征，并预判未知安全问题。这也意味着，保护较大规模的网络架构所需的人员数量正在减少，而应对网络攻击的措施也会更加迅速和准确。

与此同时，安全工具和服务也在转向云端，这意味着企业与服务供应商之间的信任在未来会变得非常重要。

4 主动防御与被动防御



随着网络安全攻击的成本和规模增加，企业已然无法再承受被动防御网络安全所付出的代价。相反地，Yahya认为采取一种更可预测的方法，反客为主，将会是未来的发展趋势。“企业可以对当前流量数据进行分析，网络安全专业人员可以制作模型来告知企业将来潜在的攻击问题，以及应该如何规避风险。”Yahya解释说。

Nepal也持相同看法。“基础架构的数字模型可以模拟现实世界发生的情况，（并）让你可以从攻击者的角度考虑问题，尝试用不同的攻击方式来攻击真实的系统，因为这些模型是对真实系统的复制。”

这种主动性也在评估和招聘人才过程中有所体现。Yahya是几家网络安全相关认证机构的官方指导师。他一直在推动企业的首席信息安全官（CISO）衡量候选人除技术能力以外的思维能力，这样他们的企业才能采取更主动、更全面的网络安全防御方法。

面临的威胁很有适应性，还会不断变化。企业需要持续不断地重新评估自己的计划是否可行，这需要领导技能才能实现。这就是为什么监管、风险和合规必须纳入每一位网络安全人员的日常工作。”



Faisal Yahya

上市公司Vantage Point Security印尼总经理

解读常见的网络安全威胁

恶意软件



“恶意软件”通常会在用户点击可疑链接或邮件附件时，通过漏洞打开某个网络。进入系统后，该恶意软件可以阻止访问网络的关键组件、安装有害软件或获取敏感信息。

钓鱼软件



这指的是伪装成可靠来源的欺骗性交流，目的是窃取敏感数据，例如登录信息和信用卡信息。

拒绝服务攻击



这种攻击会通过虚假请求占用整个系统、服务或网络，从而阻止通过合法请求，最终导致整个服务崩溃。

SQL注入



结构化查询语言（SQL）注入是指攻击者将恶意代码插入服务器，然后迫使它泄露敏感信息

中间人攻击



这一般发生在不安全的公共无线网络中，攻击者会插入你的设备和网络之间，然后迅速盗取你的所有个人数据。

5 以人为本的网络安全方法



“不存在万无一失的解决方案。我们每天的努力最多只能达到99%。”Yahya承认，最后的1%，也就是最薄弱的节点，很不幸就是我们人类自身。对此，Nepal表示赞同，“大部分网络安全的妥协都是人为造成的，在这个领域，技术解决方案成效有限。”。因此，网络安全领域的一个趋势就是更加关注网络安全生态系统中的人。

例如，Yahya解释说，虽然人类容易犯错，但是我们依然是防御这些攻击的第一道防线。“对员工进行教育不仅可以改善安全性，而且同时还能将网络安全所需的投资降到最低。”他说，“我们不能只关注技术层面，而是需要采取全面的方法。就是将基础架构以及员工归纳在一起，统筹规划。”

Parekh认为用户感知是网络安全的关键。“黑客现在会尝试模仿用户互动对象的ID，从而提高成功诱骗用户点击的几率。因此我们会培训员工识别这些趋势，并确认是否存在异常情况。”他解释说，“当我收到同事邮件问我‘你能帮我看看这封邮件吗？’的时候，我会很开心。这意味着他们对这封邮件心存疑惑，这有时候是件好事。”

Nepal赞同道，“从以人为本的角度来实施网络安全方案极其重要。企业的新进员工通常都会参加入职培训。但这中间并不包含网络安全的培训。员工需要有更强的网络安全意识，并了解如何在组织内保持良好的网络安全习惯，这样才能确保所有员工训练有素。解决方案应当做到无迹可寻、难以侵入。”



“网络安全就是保险。你为什么要买保险？因为万一出现问题，你希望有一张安全毯，网络安全也是一样的作用。你实施安全措施不是因为你希望出现安全事故，而是因为万一真的发生事故，你希望这些处理流程已经就位。而不是在事故之后才补救。你承担不起那样的代价。”

Dhillon Andrew Kannabhiran

Hack in the Box (HITB) 创始人兼首席执行官

洞察

网络安全招聘趋势



Celest Wen

米高蒲志深圳办公室
技术招聘经理

“现在的趋势是很多高级研究人员正在加入商业组织，搭建自己的网络安全团队。具备相关网络安全技能的海外人才也开始回国就职。企业招聘门槛正在提高，对人才学历背景、安全技术实力、产品落地和项目经验都有诸多要求。”



Houda El Fatni

米高蒲志日本技术（商务）
管理顾问

“市场亟需网络安全人才，因此客户必须强调自己的雇主价值主张。要着重介绍你们的福利待遇和职业发展机遇来吸引和留任市场上的一流人才。”

6 安全威胁重重, 应对措施也在逐步发展



据研究, 自2014年以来, 网络安全泄露事件增加了67%, 每次泄露造成的平均损失为392万美元, 这个趋势实在令人担忧。不过, 网络安全相关的机遇也在增加。在Nepal所在的澳大利亚, 网络安全形势在过去五年已经大有好转。

例如, 政府正在配置更多资源用于增强网络安全生态系统, 包括研究、创新、防御和学术等支持。举个例子, 澳大利亚政府去年八月开始实施网络安全战略2020, 将会投资16.7亿澳元用于加强安全和执法能力, 协助各行业保护企业安全, 提升全社会对线上安全的了解。

其他亚太地区的国家也在增加这方面的投入。根据《德勤网络智能指数2020》, 新加坡、韩国、澳大利亚和新西兰在网络准备方面得分最高, 表现为“强有力的数字化法规和较高的研究和开发比率, 标志着对网络安全事件具有成熟的应对能力。”排名第一的新加坡甚至在2018年宣布设立一项3000万美元的基金, 用于激励本地企业优先升级安全应对措施。不过在网络安全资金投入方面, 中国政府在亚太地区遥遥领先, 2019年该项支出达79亿美元, 仅次于美国, 位居世界第二。至于全球范围的支出, 国际数据公司预计到2024年, 全球网络安全支出将会超过1747亿美元。

洞察

网络安全招聘趋势



KYLE BURNETT

米高蒲志澳大利亚
技术经理

“网络安全一直都是SEEK和领英数据统计的全国人才需求增长最多的前五大职能领域之一。这个新兴领域对人才的需求量很大, 不过, 现在看到了庞大的毕业生人才库, 以及希望跨行业发展的的人才。我们合作的企业在招聘网络安全人才时看重的是简历上与众不同的地方。持有国际信息系统审计协会 (ISACA) 等权威机构颁发的证书, 在Cyber CX等企业的实习经历, 或者自行设计安全项目等, 都是有利的例证。”



RYAN FAULDS

米高蒲志网络和信息
安全高级顾问

“澳大利亚对网络安全人才的需求增加, 与此同时, 恶意行为也在增长。与技术领袖会面后, 我们得知各个领域都缺少网络安全人才。如果企业亟需网络安全技能, 请思考市场上的候选人会受到哪些因素驱动? 我们发现一个趋势, 优秀人才会加入那些提供学习和发展机遇、拥有积极灵活的团队文化的组织。在招聘时, 要考虑网络安全市场表现的本质, 以及可转移技能的重要性。”

网络安全领域热门招聘趋势

1 亟需高端技能



“网络安全行业的各个层级都存在技能缺口。仅研究领域，人才就非常紧缺，我们看到澳大利亚的网络安全研究人员较为匮乏。”Nepal说。“公共领域方面的缺口更多，政府机构正在努力招聘高端人才。”

中国也面临同样的情况。阮有明介绍说，网络安全是近几年才开始在中国蓬勃发展，前几年大部分中国大学甚至还没有开设相关课程。这导致市场亟需大量一流网络安全人才，尤其是能够从头开始搭建网络安全架构的人才。“正如一些重要的市场报告所展示的，人才短缺是阻碍国内外企业发展的主要因素之一。”米高蒲志深圳办公室技术招聘经理Celest Wen解释说。

面临人才问题的国家并非只有澳大利亚和中国。Kannabhiran所在的企业与全球各国政府合作，他认为人才紧缺的问题在全球范围内普遍存在。“教育系统出问题了。全世界（的企业都在）网罗网络安全精英人才，但是找不到，因为大学教育培养的人员大都不符合要求。”他感叹道，“企业不得不保留这些员工，派他们参加技能进修，花费额外开支，甚至建立企业内部测试与研究方法。”

面对这样的问题，企业应该如何应对呢？阮有明认为，至少在短期内，只能寻找海外人才。

“我建议高端人才靠引进。”他说，“中级人才靠企业内部培养。”Nepal也预计对高级人才的需求只会日益强烈，因为假以时日，低端技能最终会被人工智能取代，这意味着在短期课程中学到的技术和能力无法满足长期需求。

2 亟需软性技能



网络安全是一个高度合作型职位，因此Yahya认为合格的人才应当具备的首要软性技能是沟通和写作能力。网络安全人员不仅需要互相学习，而且还需要向不同层级和部门的利益相关者“营销”网络安全的重要性。对于Yahya来说，这些是目前极度匮乏却又极为关键的软性技能。

另外一项亟需的软性技能是成长型思维。对网络安全人员的要求会随着网络安全问题的演变而不断变化。事实上，据Yahya说，一名网络安全人员通常需要三到五年的时间才能精通某一个领域的专业知识，但是网络安全威胁的发展速度可谓日新月异。因此，拥抱变化、拥有适应性思维非常关键。“这并不是指个人成长，而是需要你敞开心胸接受反馈、接受建议、为企业打造适合的架构。”他强调说。

3 将网络安全领导视为战略合作伙伴



“作为网络安全领导，你需要理解的一点是，安全和业务必须相辅相成、互相促进。你一定不能站在业务发展的对立面，而是要从业务的角度去思考问题。”阮有明说，“只有这样，你才会知道什么时机布局网络安全最为合适，需要选择哪种网络安全措施。”

Yahya则更进一步。“在印尼，对考虑跳槽的网络安全人员来说，薪酬并不是最重要的。重要的是一个组织整体对首席信息安全官这个职位



网络安全不同于AI或区块链。它不是给业务赋能，而是保护业务不受损害，解决内部安全问题。”

阮有明

深信服科技股份有限公司首席安全架构师



的接受程度。实际上，薪酬的影响微乎其微。这些网络安全人才想了解的是业务部门是否能与他或她开展合作。吸引和留任一流网络安全人才的一种方法是将他们定位为战略合作伙伴。让他们参与决策过程。如果得不到其他职能部门的合作，他们的离职率就会非常高。”

Cipla全球财务总裁Kedar Upadhye认为自主权对于人才留任率很关键。“就是拥有思考和运作的自由。我们应该授予（合格的网络安全领导）自主权来安排事务、制定路线图及相应的预算。我们应该尊重个体的专业知识和技能。”

4 更加关注雇主品牌



合格的网络安全人员本来就可遇不可求。在谈到吸引和留任精英中的精英时，阮有明有一些想法。“首先要建立强有力的雇主品牌和积极的团队文化。”他说，所谓的“积极的团队文化”指的是雇主必须提供一个强有力的平台，让人才可以尝试网络安全的不同垂直领域。“作为领导，要给人才提供发展空间，帮助他们实现自身价值。”他解释说，“短期吸引人才可能需要靠薪资，但是长期来看，还是要靠领导风格。”

非常感谢澳大利亚联邦科学与工业研究组织 (CSIRO) Data61 首席科学家兼 Data61 分布式系统安全部门课题组长 Surya Nepal、上市公司 Vantage Point Security 印尼总经理 Faisal Yahya、深信服科技股份有限公司首席安全架构师阮有明、Hack in the Box (HITB) 创始人兼首席执行官 Dhillon Andrew Kannabhiran、Cipla 副董事 Viren Parekh、Cipla 全球财务总裁 Kedar Upadhye 热情分享的真知灼见。

PAGEGROUP

关于网络安全领域的招聘建议



MIKE SIERRA

米高蒲志菲律宾
高级技术顾问

“在招聘安全人才时，企业应该摆脱定势思维，给候选人带来优越的体验非常重要。一开始就介绍企业品牌故事和宗旨会让你们在人才竞争对手中脱颖而出。”



DANNY GOH

米高蒲志马来西亚
技术经理

“招聘经理需要了解企业内部的网络安全漏洞，以便了解需要招聘的对口人才。实际上，他们必须做好准备介入提供相关培训。最重要的一点是，找到愿意在网络安全领域成长的人。”



SHINJIKA SHUKLA

米高蒲志新加坡技术副总裁

“众所周知，数字化转型类职位普遍面临人才短缺的问题。因此，很重要的一点是，雇主主要转变思维模式，从招聘即插即用型人才转向招聘具有适当的能力、态度和技术基础的人才。”

关于Michael Page技术招聘业务

Michael Page深知招聘技术专业人员的复杂性。我们的服务兼具专业技术猎头公司的专业技能与国际猎头公司的资源、可靠性和专业度。



12 个

市场



46%

的职位为灵活用工职位



172 名

技术相关职位专业顾问



2020年,

1,700 多个

技术职位完成理想招聘



318,000 份

技术领域求职者职位申请表



我们的亚太数据库中有超过

370,000

名合格的技术人才数据

我们的招聘涵盖各大技术领域



领导力



数据、分析与商业智能



新兴技术



软件开发



交付与转型



销售



产品开发



基础设施与运营

关于PageGroup

PageGroup是全球领先的专业人才招聘公司，市值超过10亿英镑。我们是在伦敦证券交易所上市的FTSE 250指数成份股公司，目前拥有逾 7,700 名员工，在36个国家/地区设有140个办事机构。我们一直保持稳健发展，每家PageGroup办事机构均由员工亲自建立并遵循企业共同的最佳实践和价值观。

我们在亚太地区拥有最广泛、最准确的求职数据库，具有无可比拟的全球搜索能力。我们的顾问是拥有真材实料的业务专家。我们促进团队氛围，鼓励顾问人员将关注点放在发展长期业务关系上，而非一次性的佣金。

中国大陆

北京、上海、广州、深圳、苏州和成都

enquiries@michaelpage.com.cn
www.michaelpage.com.cn

香港地区

香港岛

enquiries@michaelpage.com.hk
www.michaelpage.com.hk

台湾地区

台北

enquiries@michaelpage.com.tw
www.michaelpage.com.tw

澳大利亚

悉尼、查茨伍德、帕拉玛塔、堪培拉、墨尔本、格伦威弗利、布里斯班、珀斯

enquiries@michaelpage.com.au
www.michaelpage.com.au

印度尼西亚

雅加达

enquiries@michaelpage.co.id
www.michaelpage.co.id

印度

孟买、德里和班加罗尔

enquiries@michaelpage.co.in
www.michaelpage.co.in

日本

东京

enquiries@michaelpage.co.jp
www.michaelpage.co.jp

马来西亚

吉隆坡

enquiries@michaelpage.com.my
www.michaelpage.com.my

新加坡

enquiries@michaelpage.com.sg
www.michaelpage.com.sg

泰国

曼谷

enquiries@michaelpage.co.th
www.michaelpage.co.th

越南

胡志明市

vnenquiries@michaelpage.com.vn
www.michaelpage.com.vn

菲律宾

马尼拉

phenquiries@michaelpage.com.ph
www.michaelpage.com.ph

亚洲其他地区

服务于东盟地区，包括缅甸

enquiries@michaelpage.com.my
www.michaelpage.com.my

PageExecutive

MichaelPage

PagePersonnel

PageOutsourcing

Part of
PageGroup

“科技ABC人才发展系列”是Michael Page独家推出的技术领域专题系列报告,探索人工智能、区块链、网络安全和大数据这四大高增长技术领域的最新技术创新与招聘趋势。每份报告都涵盖亚太地区技术专家、商业领袖和Michael Page招聘顾问的见解和建议。想了解更多技术领域的发展方向和关键技能,您可以下载阅读报告,或者访问您所在国家/地区的Michael Page官方网站。

